

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF:
INFORMATION ASSOCIATED WITH

NOTSOLEANEILEEN@GMAIL.COM
KEWLMARGOD@GMAIL.COM
WILEYKYLIHUNT@GMAIL.COM

Mag. No. 19-720M
[UNDER SEAL]

THAT ARE STORED AT PREMISES CONTROLLED BY
GOOGLE, LLC. AT 1600 AMPHITHEATRE PARKWAY,
MOUNTAIN VIEW, CALIFORNIA 94043

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Katherine Donohue, a Special Agent (SA) with the Federal Bureau of Investigation, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), currently assigned to the Pittsburgh, Pennsylvania office. I have been so employed since June 2016. As part of my duties, I investigate violations of federal law, including the online exploitation of children, which includes violations pertaining to the illegal possession, receipt, transmission, and production of material depicting the sexual exploitation of minors, among other. I have gained expertise in conducting such investigations through training in the area of child pornography and child exploitation investigations in seminars, classes, and everyday work related to conducting these types of investigations, and have had the opportunity to observe and review numerous examples of child pornography in a variety of media, including computer/electronic media. I have obtained FBI Basic and Advanced Crimes Against Children Training. I have participated in the execution of numerous federal and state search warrants, which have involved child sexual exploitation and/or child pornography offenses. By virtue of my position, I perform and have

performed a variety of investigative tasks, including the execution of federal search warrants and seizures, and the identification and collection of computer-related evidence.

2. The facts set forth in this affidavit are based on my personal knowledge, information obtained during my participation in this investigation, knowledge obtained from other individuals, including other law enforcement personnel and computer forensic examiners, review of documents and records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience.

3. I know that Title 18, United States Code, Section 2252(a) makes it a crime to knowingly possess, receive and/or distribute a visual depiction of a minor engaged in sexually explicit conduct, as defined in Section 2256 of Title 18, when such visual depiction has either been transported or shipped in interstate or foreign commerce.

4. As will be shown below, there is probable cause to believe that evidence of violations of Title 18, United States Code, Section 2252(a) as further described in Attachment A hereto, is stored at the premises controlled by Google, Inc.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. This affidavit is submitted in support of an application for a search warrant for information contained in or associated with the Google, LLC electronic mail (e-mail) accounts of **kewlmargod@gmail.com**, **notsoleaneileen@gmail.com**, and **wileykilihunt@gmail.com**, controlled by the web-based electronic communication service provider known as Google, LLC,

headquartered at 1600 Amphitheater Parkway, Mountain View, CA 94043. The location to be searched is particularly described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Google, LLC to disclose to the government copies of records, images, and other information, (including the content of communications), as particularly described in Attachment B, associated with the accounts **kewlmargod@gmail.com**, **notsoleaneileen@gmail.com**, and **wileykilihunt@gmail.com**.

7. Your Affiant is requesting authority to search the account and its associated applications, to include but not be limited to Google Photos, where the items, specified in Attachment A, may be found, and to seize all items listed in Attachment B as evidence, fruits, and/or instrumentalities of violations of Title 18, United States Code, Section 2252(a).

8. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. 2711. Specifically, the Court is a “district court of the United States that has jurisdiction over the offense being investigated.” 18 U.S.C. 2711(3)(A)(i).

9. The statements in this affidavit are based, in part, on information provided by witnesses and your Affiant’s investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause.

DEFINITIONS

10. The following definitions apply to this Affidavit:

a. “Child Erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. “Child Pornography,” as used herein, includes the definitions in 18 U.S.C. 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual, the production of which involves the use of a minor engaged in sexually explicit conduct (see 18 U.S.C. 2252 and 2256(2)).

c. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. 2256(5).

d. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. 2256(2).

e. “Computer,” as used herein, is defined pursuant 18 U.S.C. 1030(e)(1), as

“an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”

f. “Minor” means any person under the age of eighteen years. See 18 U.S.C. 2256(1).

g. “Internet Service Providers” (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an “email address”, an email mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password. ISPs maintain records (“ISP records”) pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), email communications, information concerning content uploaded

and/or stored on or via the ISPs servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscriber's use. This service by ISPs allows for both temporary and long term storage of electronic communications and many other types of electronic data and files. Typically, email that has not been opened by an ISP customer is stored temporarily by an ISP incident to the transmission of that email to the intended recipient, usually within an area known as the home directory. Such temporary, incidental storage is defined by statute as "electronic storage," see 18 U.S.C. 2510(17), and the provider of such service is an "electronic communication service."

h. An "electronic communication service," as defined by statute, is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. 2510(15). A service provider that is available to the public and provides storage facilities after an electronic communication has been transmitted and opened by the recipient, or provides other long term storage services to the public for electronic data and files, is defined by statute as providing a "remote computing service." 18 U.S.C. 2711(2).

i. "Domain names" are common, easy to remember names associated with an Internet Protocol address. For example, a domain name of "www.usdoj.gov" refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level, or top-level domains, are typically .com for commercial organizations, .gov for government organizations, .org for organizations, and .edu

for educational organizations. Second level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States Government.

j. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet.

PROBABLE CAUSE

11. On February 6, 2019, the Western Pennsylvania Violent Crimes Against Children Task Force (WPVCAC TF), executed a search warrant at the residence of 50 Vanadium Road, Apt. 137, Bridgeville PA, 15017 as a result of a National Center for Missing and Exploited Children (NCMEC) Cybertip received from Google. Google reported that on May 1, 2018 and May 4, 2018, a user using the email address gretskicarol@gmail.com from internet protocol (IP) address 2601:547:1280:69b4:5d72:7adf:f39f:17f9 uploaded the same image of a nude prepubescent female, approximately 5-6 years old, exposing her genitals in a sexual act and/or pose. The aforementioned IP address resolved to Comcast. On September 25, 2018, a search warrant issued in the Pennsylvania Court of Common Pleas was served on Comcast for IP address 2601:547:1280:69b4:5d72:7adf:f39f:17f9. On October 10, 2018, Comcast responded to the

search warrant and provided subscriber name of Paul Chretien with subscriber address 50 Vanadium Rd Apt 137, Bridgeville PA, 15017, telephone number (207) 458-5506, and account number 8993210070310666.

12. On February 6, 2019, during the execution of the search warrant at 50 Vanadium Rd., Apt 137, Bridgeville PA, 15017, Paul Chretien (hereinafter referred to as Chretien), was interviewed and consented to law enforcement taking over his online presence, which included more than 28 different gmail email accounts. During the voluntary, non-custodial interview, Chretien consented to agents taking over multiple email accounts that he used to assume the identity of a minor female and engage with other users in Google Hangouts. Chretien signed a “consent to Assume Online Presence” form, provided the agents with the password(s) to his accounts, and gave consent for your Affiant to take over his numerous email accounts and change the passwords.

13. Chretien informed investigators that he sought other individuals who “enjoy doing things to young people” to talk to in Google Hangouts, and this included conversations with others about “horror and violence.” Chretien stated that he would send and receive images during the Google Hangout chats. The images were of both clothed females and young nude females.

14. Chretien further told investigators that he had been chatting with a Google Hangouts user: craig.foster815@gmail.com for approximately ten years. Chretien and craig.foster815@gmail.com shared an affinity for “the female abdomen”, including violence to the abdomen.

15. On February 7, 2019, utilizing a government computer and internet source, your

Affiant successfully logged into 28 of Chretien's gmail accounts and changed Chretien's passwords so that Chretien would be unable to delete or alter the contents of the accounts. The accounts have been in your Affiant's control since then.

16. On February 12, 2019, a preservation letter was issued to Google LLC for Chretien's 28 gmail accounts.

17. Since February 7, 2019, I have periodically logged into and reviewed the contents of Chretien's accounts. I have found the following: Chretien, using several different Google accounts, chatted with an individual within Google Hangouts with the display name "Craig Foster" and email address: craig.foster815@gmail.com (hereinafter "Craig Foster"). In each Google Hangouts chat session between Chretien and Craig Foster reviewed by your Affiant and discussed herein, Chretien would portray himself as a minor female. At the start of each chat session, Chretien would state his purported age to Craig Foster, typically stating that he was between the ages of five and twelve. During the chats, Chretien would send images of prepubescent females and pretend to be the girl depicted in those images. While using this assumed identity, the first image Chretien sent to Craig Foster usually was that of a minor female clothed in a bathing suit. In certain chat sessions, images exchanged between the two also included images of child pornography.

18. On March 1, 2019, your Affiant logged onto Chretien's accounts and reviewed Google Hangouts communications between Chretien and Craig Foster:

- a. On August 22, 2018, Chretien used the email address **notsoleaneileen@gmail.com** to communicate with Craig Foster

(craig.foster815@gmail.com) in Google Hangouts. On this date, Craig Foster sent an image of a nude female under the age of 18 years old, exposing her genitals to the camera to Chretien and stated: “I want to be the first to have my fingers in your pussy.”

- b. On September 26, 2018, Chretien used the email address **kewlmargod@gmail.com** and communicated with Craig Foster in Google Hangouts. On that date, Chretien sent to Craig Foster 8 images of nude prepubescent females, approximately 5 to 7 years old, exposing their genitals to the camera; user craig.foster815@gmail.com (“Craig Foster”) sent one of the images that Chretien had sent to him back to Chretien—an image of a nude prepubescent female, approximately 5-6 years old, exposing her genitals to the camera.
- c. On November 11, 2018, Chretien used the email address wileykylihunt@gmail.com to communicate with Craig Foster in Google Hangouts. On this date, Chretien sent to Craig Foster (craig.foster815@gmail.com) 3 images of a nude prepubescent female, approximately 5-6 years old, exposing her genitals to the camera. In response, Craig Foster (craig.foster815@gmail.com) sent an image of an adult penis and stated: “That’s me . . . right now . . . “

19. While logged into Chretien’s accounts, your Affiant also has observed recent attempts by Craig Foster in Google Hangouts to communicate with Chretien at other email

addresses belonging to Chretien (stacyjisok@gmail.com and mary4scarystuff@gmail.com), asking: “Do you ever come on here anymore?” and stating, “I miss chatting with you.”

20. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain the contents of the subject accounts by other means.

21. Based on my review of the aforementioned Google email accounts and Google Hangout communications between Chretien via his numerous gmail accounts and Craig Foster, I know that Chretien possessed and distributed images in violation of Title 18, United States Code, Section 2252(a).

BACKGROUND REGARDING EMAIL AND THE PROVIDER

22. In my training and experience, I have learned that Google, LLC provides a variety of services to the public, including email and free online storage space.

23. Google, LLC provides its subscribers internet-based accounts that allow them to send, receive, and store e-mails online. Google, LLC accounts are typically identified by a single username, which serves as the subscriber’s default e-mail address, but which can also function as a subscriber’s username for other Google, LLC services, such as instant messages and remote photo or file storage.

24. Google, LLC’s online storage service is known as “Google Drive,” and is a file storage and synchronization service. Google Drive allows users to store files remotely on Google servers, synchronize files across devices, and share files. It is available on the Internet and as a mobile application. Files and folders stored in Google Drive can be shared privately with other users having a Google services account.

25. Google Photos is a photo sharing and storage service developed by Google and is available both on the Internet via website and as a mobile application. Google Photos gives users free unlimited storage space for photos and videos, under certain conditions, described below. Google Photos can be configured to automatically sync photos and videos taken with a user's camera to a user's Google Photo account. Like Google Drive, Google Photos allows users to store files remotely on Google servers, synchronize files across devices, and share files.

26. Google Drive and Google Photos are complementary parts of the same Google services account. Photos and videos are stored on a user's Google account's storage space with each account having 15 gigabytes (GB) of free storage, with the option to purchase additional storage space. Files uploaded to a user's Google account via Google Drive count against the 15 GB quota. Files uploaded via Google Photos do not count against the account's quota as long as they are uploaded as "High Quality" (Google's term). Google advertises that images/videos uploaded as "High Quality" get an unlimited amount of storage space. Images/videos uploaded in "Original Quality" (Google's term) do count against the account's quota. The difference between "High Quality" and "Original Quality" has to do with the amount of compression applied to a file, which affects the file's size.

27. The Google Photos mobile application is configured to automatically transfer and store graphics files created on the mobile device to the Google Photos service associated with the Google account. Users also have the option to manually transfer files between Google Photos and Google Drive.

28. Google, LLC allows subscribers to obtain Google Drive storage space at the domain name “gmail.com.” Subscribers obtain an account by registering with Google, LLC. During the registration process, Google, LLC asks subscribers to provide basic personal information such as a name, an alternate e-mail address for backup purposes, a phone number, and, in some cases, a means of payment. Google, LLC typically does not verify subscriber names. However, Google, LLC does verify the e-mail address or phone number provided. Therefore, the computers of Google, LLC are likely to contain stored information concerning subscribers and their use of Google, LLC services, such as account access information and account application information.

29. Once a subscriber has registered an account, Google, LLC provides e-mail services that typically include folders such as an “inbox” and a “sent mail” folder, as well as electronic address books or contact lists, and all of those folders are linked to the subscriber’s username. Google, LLC subscribers can also use that same username or account in connection with other services provided by Google, LLC.¹ Notably, for the purposes of this investigation and this

¹ THESE SERVICES MAY INCLUDE: electronic communication services such as Google Voice (voice calls, voicemail, and SMS text messaging), Hangouts (instant messaging and video chats), Google+ (social networking), Google Groups (group discussions), Google Photos (photo sharing), and YouTube (video sharing); web browsing and search tools such as Google Search (internet searches), Web History (bookmarks and recorded browsing history), and Google Chrome (web browser); online productivity tools such as Google Calendar, Google Contacts, Google Docs (word processing), Google Keep (storing text), Google Drive (cloud storage), Google Maps (maps with driving directions and local business search) and other location services, and Language Tools (text translation); online tracking and advertising tools such as Google Analytics (tracking and reporting on website traffic) and Google AdWords (user targeting based on search queries); Pixel Phone (services which support a Google smartphone); and Google Play (which allow users to purchase and download digital content, e.g., applications).

application, Google, LLC also provides “cloud” storage services. Account holder/users can utilize this service, which is called “Google Drive,” to store pictures, videos, and other electronic files remotely and without taking up memory space on their personal computer, smart phone, and physical storage media.

30. In general, files that are transferred to a Google Drive or Google Photos account are stored in the subscriber’s storage space on Google, LLC servers until the subscriber deletes the data. If the subscriber does not delete files, they can remain on Google, LLC servers indefinitely. Even if the subscriber deletes files, they may continue to be available on Google, LLC’s servers for a certain period of time.

31. A Google, LLC subscriber can also store files in addition to graphics, such as address books, contact or buddy lists, calendar data, and other files on servers maintained and/or owned by Google, LLC via the Google Drive service.

32. Google, LLC typically retains certain transactional information about the creation and use of each account on their system. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), and other log files that reflect usage of the account. In addition, Google, LLC logs and retains the Internet Protocol address (“IP address”) used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which devices were used to access the relevant account. Also, providers such as Google, LLC typically collect and maintain

location data related to subscriber's use of Google, LLC services, including data derived from IP addresses and/or Global Positioning System ("GPS") data.

33. Based on my training and experience, I know that providers such as Google, LLC also collect information relating to the devices used to access a subscriber's account – such as laptop or desktop computers, cell phones, and tablet computers. Such devices can be identified in various ways. For example, some identifiers are assigned to a device by the manufacturer and relate to the specific machine or "hardware," some identifiers are assigned by a telephone carrier concerning a particular user account for cellular data or voice services, and some identifiers are actually assigned by Google, LLC in order to track what devices are using Google, LLC's accounts and services. Examples of these identifiers include unique application number, hardware model, operating system version, Global Unique Identifier ("GUID"), device serial number, mobile network information, telephone number, Media Access Control ("MAC") address, and International Mobile Equipment Identity ("IMEI"). Based on my training and experience, I know that such identifiers may constitute evidence of the crimes under investigation because they can be used (a) to find other Google, LLC accounts created or accessed by the same device and likely belonging to the same user, (b) to find other types of accounts linked to the same device and user, and (c) to determine whether a particular device recovered during course of the investigation was used to access the Google, LLC account.

34. Based on my training and experience, I know that Google, LLC maintains records that can link different Google, LLC accounts to one another, by virtue of common identifiers, such as common e-mail addresses, common telephone numbers, common device identifiers, common

computer cookies, and common names or addresses, that can show a single person, or single group of persons, used multiple Google, LLC accounts. Based on my training and experience, I also know that evidence concerning the identity of such linked accounts can be useful evidence in identifying the person or persons who have used a particular Google, LLC account.

35. Based on my training and experience, I know that subscribers can communicate directly with Google, LLC about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers such as Google, LLC typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

36. In summary, I know that Chretien's email accounts are associated with numerous Google, LLC services, including Google Photos and Google Drive. Based on my training and experience in this context, I believe the servers of Google, LLC are likely to contained user-generated content such as stored electronic communications (including retrieved and unretrieved e-mail for Google, LLC subscribers), as well as Google, LLC-generated information about its subscribers and their use of Google, LLC services and other online services. In my training and experience, all of that information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. In fact, even if

subscribers provide Google, LLC with false information about their identities, that false information often nevertheless provides clues to their identities, locations, or illicit activities.

37. As explained above, information stored in connection with a Google, LLC account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element of the offense, or, alternatively, to exclude the innocent from further suspicion. From my training and experience, I know that the information stored in connection with a Google, LLC account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, e-mail communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by Google, LLC can show how and when the account was accessed or used. For example, providers such as Google, LLC typically log the IP addresses from which users access the account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the Google, LLC account access and use relating to the criminal activity under investigation. This geographic and timeline information may tend to either inculcate or exculpate the person who controlled, used, and/or created the account. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via e-mail). Finally, stored electronic data may provide relevant insight into the user’s state of mind as it relates

to the offense under investigation. For example, information in the Google, LLC account may indicate its user's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

38. All of the above facts and circumstances, taken together, lead your Affiant, based on her training and experience, to believe that evidence of the offenses under investigation is located, stored, or contained in the Google, LLC account associated with the email addresses **kewlmargod@gmail.com**, **notsoleaneileen@gmail.com**, and **wileykilihunt@gmail.com**, including sexually explicit images and/or videos of minors. These images and/or videos and any other associated information, such as exif information or other information about when such images/videos were made, shared, and/or "backed up," constitute evidence, instrumentalities, fruits, and contraband associated with the specified violations.

39. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google, LLC to disclose to the government copies of the items and information (including the content of communications) particularly described in Section I of Attachment B.

SEALING ORDER REQUESTED

40. It is further respectfully requested that this Court issue an Order sealing, until further order of this Court, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant and the requisite inventory notice (with the exception of one copy of the warrant and inventory notice that will be sent to Google). Sealing is necessary

because the items and information to be seized are relevant to an ongoing investigation and premature disclosure of the contents of this Affidavit and related documents may have a negative impact on the continuing investigation and may otherwise jeopardize its effectiveness.

CONCLUSION


41. Based on the information set forth above, your affiant respectfully submits that there is probable cause to believe that located within the following Gmail accounts: **kewlmargod@gmail.com**, **notsoleaneileen@gmail.com**, and **wileykilihunt@gmail.com**, stored at the premises controlled by Google, Inc., at 1600 Amphitheatre Parkway, Mountain View, CA, 94043, there is evidence, fruits, and instrumentalities of the above-described violations of Title 18, United States Code, Section 2252(a), more specifically described in Attachment A to this affidavit, which is incorporated herein by reference. Accordingly, I request that the Court issue the proposed search warrant.

42. Your Affiant respectfully requests that a warrant be issued authorizing the search of the Gmail accounts: **kewlmargod@gmail.com**, **notsoleaneileen@gmail.com**, and **wileykilihunt@gmail.com**, and each account's related Google applications, to include Google Photos, and authorizing the seizure of the items listed in Attachment B, hereto.

43. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

44. The above information is true and correct to the best of my knowledge, information and belief.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Katherine Donohue', written over a horizontal line.

Katherine Donohue
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
this 2 day of April, 2019.

A handwritten signature in black ink, appearing to read 'Lisa Pupo Lenihan', written over a horizontal line.

THE HONORABLE LISA PUPO LENIHAN
~~Chief~~ United States Magistrate Judge

ATTACHMENT A

Property/Location to Be Searched

The property/location to be searched is the Google, LLC account identified by and/or associated with the email accounts/addresses: **kewlmargod@gmail.com**, **notsoleaneileen@gmail.com**, and **wileykilihunt@gmail.com**, which are known by law enforcement to be associated with PAUL CHRETIEN and which are stored and maintained at premises owned, maintained, controlled, or operated by Google, LLC, a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google, LLC:

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, LLC, regardless of whether such information is located within or outside of the United States, and including any records or information that have been deleted but are still available to Google, LLC, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google, LLC is required to disclose the following information to the government for the account or identifier listed in Attachment A, for the time period of August 1, 2018 to the present:

- (a) The content of all communications sent to or from the account (including through Gmail, Google Hangouts (including videos, and otherwise), stored in draft form in the account, or otherwise associated with the account, including all message content, attachments, and header information;
- (b) All address book, contact list, or similar information associated with the account;
- (c) All contact and personal identifying information, including full name, user identification number, birth date, contact e-mail addresses, passwords, security questions and answers, physical address (including city, state, and zip code), telephone numbers, and screen names;
- (d) All Google Drive content;
- (e) All services used by the account;
- (f) All subscriber and payment information, including full name, email address (including any secondary or recovery email addresses), physical address (including

city, state, and zip code), date of birth, gender, hometown, occupation, telephone number, websites, screen names, user identification numbers, security questions and answers, registration IP address, payment history, and other personal identifiers;

- (g) The dates and times at which the account and profile were created, and the Internet Protocol (“IP”) address at the time of sign-up;
- (h) All transactional records associated with the account, including any IP logs or other records of session times and durations;
- (i) Any information identifying the device or devices used to access the account, including a device serial number, a GUID or Global Unique Identifier, Android ID, a phone number, serial numbers, MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”), and any other information regarding the types of devices used to access the account;
- (j) All activity logs for the account;
- (k) All photos and videos uploaded to the account, including in Google Drive and Google Photos;
- (l) All information associated with Google Plus, including the names of all Circles and the accounts grouped into them;

- (m) Google Analytics: All properties and UA codes associated with the Target Account, and for each of those properties and UA codes, all usernames and email accounts associated with them. In addition, for all properties and UA codes associated with the Target Account, all Audience Reports. For all properties and UA codes associated with the Target Account, all data uploaded by the user of the Target Account into Google Analytics.
- (n) All photos and videos uploaded by any user that have that user tagged in them;
- (o) All location information;
- (p) The types of service utilized by the user;
- (q) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (r) All privacy settings and other account settings, including email addresses or other accounts that the account has blocked;
- (s) Linked Accounts: All accounts linked to the Target Account (including where linked by machine cookie or other cookie, creation or login IP address, recovery email or phone number, AOL account ID, Android ID, Google ID, SMS, Apple ID, or otherwise);
- (t) For accounts linked by cookie, the date(s) on which they shared a cookie;
- (u) For accounts linked by SMS number, information regarding whether the numbers were verified; and
- (v) Customer Correspondence: All records pertaining to communications between the Service Provider and any person regarding the user or the user's account with the

Service Provider, including contacts with support services, records of actions taken, and investigative or user complaints concerning the subscriber.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2251(a), 2252(a)(2) and 2252(a)(4)(B) involving PAUL CHRETIEN, for each account or identifier listed on Attachment A, information, including the content of communications, internet search history, and documents, images, and videos, pertaining to the following matters: since August 1, 2018 in the form of the following:

- (a) Records and information, including photos, images, and videos, constituting, referencing, or revealing child pornography, as defined in 18 U.S.C. 2256(8);
- (b) Records and information, including photos, images, and videos, constituting, referencing, or revealing child erotica;
- (c) Records and information, including photos, images, videos, constituting, referencing, or revealing the trafficking, advertising, or possession of child pornography, to include the identity of the individuals involved;
- (d) Records and information referencing or revealing a sexual interest in children or the sexual exploitation of children, to include the identity of the individuals involved;
- (e) Records and information constituting, referencing, or revealing communication or interaction of an illicit sexual nature about a minor or with a minor, including the content of all emails and instant message communications associated with the account(s), the source and destination addresses associated with each email, the

date and time at which email was sent, and the size and length of each email, and the identity of the individuals involved;

- (f) For all items described in this section above, any images, videos, email, instant message communications, records, files, logs, current information, or information or images or videos that have been deleted but are still available to the Provider, or which have been preserved pursuant to a request to preserve the account;
- (g) For all items described above, records and other information stored at any time by an individual using the account, including address books, contact and buddy lists, pictures, and files;
- (h) For all items described in this section above, all metadata, transaction information, storage structure, and other data revealing how the items were created, edited, deleted, viewed, or otherwise interacted with;
- (i) Records and information revealing or referencing information about the device(s) used to access the account;
- (j) Records and information revealing or referencing the identity of the individual who created and used the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, devices associated with the account, the length of service, the IP address used to register the Account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- (k) Any photos, documents, or other files that may indicate user attribution or ownership of the account;

- (l) All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and
- (m) Identity of accounts linked by cookies.

As used above, “child erotica” means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions. The term “minor” means any person under the age of 18 years.

III. Delivery of Information by Google, LLC to the Federal Government

Within **14 days** of the issuance of this warrant, and notwithstanding Title 18, United States Code, Section 2252A or similar statute or code, Google, LLC shall disclose and deliver the information set forth above to the government via the United States Postal Service, another courier service, or email by sending to:

Special Agent Katherine Donohue
Federal Bureau of Investigation
3311 E Carson Street
Pittsburgh, PA 15203
kadonohue@fbi.gov

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by **Google, LLC** and my title is _____.

I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of **Google, LLC**. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of **Google, LLC**, and they were made by **Google, LLC** as a regular practice; and

b. such records were generated by **Google, LLC** electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of **Google, LLC** in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by **Google, LLC**, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature